Many thanks to our sponsors and partners!

Powered by orange

PLATINUM SPONSORS

BIT SENTINEL

3CYBER

CYBER LIFE HACKS

HACKING VILLAGE PARTNERS

cyber EDU

electron

HACKOUT Portalul Atacurilor Cibernetice

SILVER SPONSORS

efect

PFG FINANCE

wantsome the friendly IT academy

MOBILITY PARTNER

TOYOTA Cluj-Napoca prin Profi Auto

COMMUNITY & MEDIA PARTNERS

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

CLUJ IT

UNIVERSITATEA BABEȘ-BOLYAI
BABEȘ-BOLYAI TUDOMÁNYEGYETEM
BABEȘ-BOLYAI UNIVERSITÄT
BABEȘ-BOLYAI UNIVERSITY
TRADITIO ET EXCELLENTIA

BRCC British Romanian Chamber of Commerce

ISACA Trust in, and value from, information systems Romania Chapter

(ISC)² CHAPTER ROMANIA

Cloud Security Alliance Official Chapter Romania Chapter CSA

CARTEA DALIEI

x86 GENERATION

WOMEN 4CYBER EUROPEAN CYBER SECURITY ORGANISATION ROMANIA

ȘCOALA INFORMALĂ DE IT®

TSM TODAY SOFTWARE MAGAZINE

DevExperience

ITCAMP

MOBZINE.RO

SecurityPatch

ROTSA The highway of Romanian Tech Startups

techcelerator

DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

EU DIRECTIVE 2022/2555

OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on measures for a high common level of cyber security within the Union

NIS 2 DIRECTIVE

May 2024

DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

The Romanian National legal framework in Cyber Security

1) Romanian National Cyber Security Directorate founding act - Emergency Ordinance no. 104/2021, approved by the Law no. 11/2022
2) NIS Directive Transposition Law no. 362/2018
3) Government Decision no.1321/2021 – The New Romanian National Cyber Security Strategy v.2.0 for 2022-2027

Romanian National Cyber Security Directorate (DNSC)

The DNSC operates:

- **SPOC** (Single Point Of Contact) for NIS 2
- National **CSIRT** (Computer Security Incident Response Team)

Objectives in the context of the implementation of the NIS 2 Directive:

- Creation and operation of a national platform enabling the exchange of information between constituents, state institutions, industry sectors in the field of cyber incidents, vulnerabilities, crises
- Coordinate efforts to improve the overall national level of cybersecurity across all civilian fields
- Identifying challenges and opportunities specific to the Romanian cyber industry to which it will provide research and educational content services
- Preparing, coordinating and providing other state institutions with capabilities to deter and respond to cyber attacks and threats to national infrastructures

What we will talk about

- DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of security of networks and information systems across the Union (NIS)
- DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cyber security throughout the Union (NIS 2)

We will mention:

- REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience in the financial sector (DORA)
- DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities

Introduction

- Over the last decade, cyber security has become a priority for the European Union in the context of increasing cyber threats and growing reliance on technology in all aspects of economic and social life.
- Major cybersecurity incidents, such as ransomware attacks affecting critical infrastructure and financial institutions, have highlighted the need for robust regulations to protect vital infrastructure and citizens data.

Aim of the presentation:

- We analyse how the NIS 2 Directive updates and extends the regulations set out in the original NIS Directive to address new challenges and vulnerabilities in cyber security.
- We will discuss the impact of the NIS 2 Directive on organisations, including the increased obligations and compliance measures required, and the benefits of improved security for all stakeholders.

What is the NIS Directive?

- **The NIS Directive** is the first piece of legislation at EU level to address the issue of cyber security risks through the uniform implementation of cyber security measures**.**
- **Purpose**: Increase the level of cyber security at Union level.
- **Scope**: It addresses sectors considered vital to society such as energy, transport, financial-banking, health, drinking water and digital infrastructure.

What is the NIS 2 Directive?

- The NIS 2 Directive is an upgrade of the NIS Directive
- It starts from principles and tools defined in the NIS Directive
- It has a similar but stricter approach and a broader scope
- Slight differences in concepts and terminology

Implementation deadline: 17 Oct 2024

Important measures introduced by the NIS Directive:

- Member States must adopt a national strategy on network and information systems security;
- Establish a European cooperation group to increase information exchange and trust between states;
- Designation of single points of contact, vital for ensuring cooperation and coordination between states.
- Designate CSIRT teams and create a network of these teams to collaborate and exchange information, best practices, etc;
- Sets security and notification requirements;
- Designation of sectors to be covered - essential service operators and digital service providers;

Why was the NIS Directive upgrade necessary?

- Digitalisation and increased interconnectivity
- Cyber attacks are growing in number, sophistication, magnitude and impact (2019 - cybercrime has doubled)
- Large differences between countries in the transposition and application of the NIS Directive
- The need to extend the scope

What's new in the NIS 2 Directive?

- Addressing supply chain issues from a cyber security perspective
- Notification is made within well-defined deadlines (24h, 72h, one month)
- Clearer supervision and control measures
- Implementation of a coordinated vulnerability disclosure policy at national level (CVD)
- Establishing/defining national frameworks for managing large-scale incidents or cyber crises and setting up EU-CyCLONe
- Peer reviews between Member States
- Accountability of the management of key and important entities, the Board must be aware of the cyber risk management measures and monitor their implementation, being directly accountable (must attend courses to have the necessary knowledges)

EU CyCLONe:

- Increase the level of preparedness of the management of large-scale cybersecurity incidents and crises;
- Establish a network for cooperation of designated national agencies and authorities responsible for cyber crisis management;
- To support the coordinated operational management **of large-scale incidents and crises** and to ensure regular exchange of relevant information between Member States and institutions from the EU.

What's new in the NIS 2 Directive?

- Extending the scope from 7 to 18 sectors, divided into key and important entities

	Energy	Transport	Banking sector	Financial market infrastructures	Health sector	Supply and distribution of drinking water	Digital infrastructure	Waste water	Management of ICT services	Public administration	Space
NIS	X	X	X	X	X	X	X				
NIS 2	X +	X	X	X	X +	X	X +	X	X	X	X

Important sectors:

	Postal and courier services	Waste management	Manufacture, production and distribution of chemicals	Production, processing and distribution of food	Manufacture	Digital service providers	Research
NIS						X	
NIS 2	X	X	X	X	X	X +	X

Categories of businesses

European Commission Recommendation 2003/361/EC:

- Micro-enterprise with less than 10 employees and annual turnover/annual balance sheet below 2 mil Euro
- Small business with less than 50 employees and annual turnover/anuual balance sheet below 10 mil Euro
- Medium-sized enterprise with less than 250 employees and annual turnover of less than 50 million Euro or a balance sheet of less than 43 million Euro

Essential entities:

- Entities above the threshold of medium-sized entities and operating in the sectors listed in Annex I
- Qualified trust service providers and top-level domain name registries, as well as DNS service providers, regardless of their size;
- providers of public electronic communications networks or publicly available electronic communications services that qualify as medium-sized enterprises;
- public administration entities at central level;

Special cases concerning the designation of essential and important entities:

- Entities providing an essential service to society
- Entities providing services which, if disrupted, would significantly affect public safety and security or public health
- The disruption of the service provided by the entity could generate significant systemic, cross-border risk;
- The entity is critical to a particular sector at national or regional level;
- Public administration entities at central or regional level if they are of significant importance.

Of note:

- Esential entities will also include critical entities, therefore NIS 2 should be aligned with Directive (2022/2557)
- It will also include most, if not all, IT service providers to the financial sector, therefore it will also need to be aligned with the DORA Directive (2022/2554)
- Other entities may be included depending on the specificities of the Member State (local authorities, educational institutions providing critical research activities)

Cybersecurity risk management measures:

- Policies on risk analysis and information system security;
- Incident handling;
- Business continuity;
- **Supply chain security** (https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks)
- security in network and information systems acquisition,
- Policies and procedures to assess the effectiveness of cybersecurity risk management measures;
- Basic **cyber hygiene** practices **and** cyber security **training**
- Policies and procedures on the use of cryptography and encryption;
- Human resources security, access control policies and asset management
- The use of multi-factor authentication solutions, secure communications and secure emergency communications systems
- The obligation to **report** significant **incidents**

Surveillance and enforcement measures:

- On-site inspections and off-site supervision
- Regular and targeted security audits
- Ad hoc audits,
- Security scans
- Information requests
- Requests for access to data, documents and any information
- Requests for evidence of implementation of cybersecurity policies

Sanctions:

- Warnings
- Adopt binding instructions (to prevent or remedy an incident)
- Enforcing the implementation of cybersecurity measures within well-defined deadlines
- Inform clients in order to mitigate the attack
- Application of sanctions
  - Esential entities - up to €10 million or 2% of worldwide turnover
  - Important entities - up to 7 million Euro or 1.4% of worldwide turnover
- Temporarily suspend a certification or authorisation concerning part or all of the relevant services provided or activities carried out
- Temporarily prohibit exercising managerial functions

Conclusions:

- Extending the scope
- Significant incident reporting obligations are defined
- Security measures are defined, being a risk-based approach
- Clearer supervision and control measures are established
- Enforcement measures are established

Q&A

Thank you!

Gabriel Niculescu
Legal expert policy, cybersecurity standardization
gabriel.niculescu@dnsc.ro

Notes

TLP:CLEAR = Limited disclosure, recipients can spread this within their community. Sources may use TLP:CLEAR when information is useful to increase awareness within their wider community.

Recipients may share TLP:CLEAR information with peers and partner organizations within their community, but not via publicly accessible channels.

TLP:CLEAR information may not be shared outside of the community. Note: when "community" is not defined, assume the cybersecurity / defense community.

Source: https://www.first.org/tlp/